

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003198544 A**(43) Date of publication of application: **11.07.03**

(51) Int. Cl.
H04L 9/32
G06F 15/00
G09C 1/00
H04L 9/08

(21) Application number: **2002301924**(22) Date of filing: **18.10.02**(30) Priority: **19.10.01 JP 2001321656**(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor:
YAMAMOTO MASAYA
MIURA YASUSHI
NAKAHARA TORU

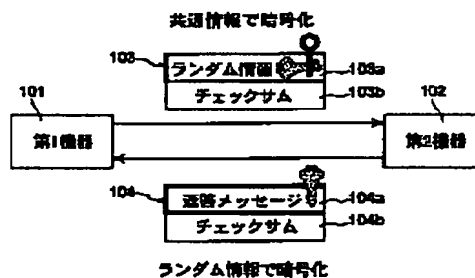
**(54) EQUIPMENT AUTHENTICATION SYSTEM AND
 EQUIPMENT AUTHENTICATION METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an equipment authentication system for certain equipment to securely specify the other equipment included in the same group as the present equipment when all the equipment are equal since it is estimated that processing such as copy or move of contents is permitted only within a certain fixed range when performing such processing among a plurality of equipments.

SOLUTION: Transmission data 103 to be transmitted from a first equipment 101 is composed of random information 103a and a checksum 103b enciphered by common information, and transmitted to a second equipment 102. The second equipment 102 receives the transmission data 103 and returns reply data 104 composed of an answer message 104a and a checksum 104b enciphered by the random information 103a to the first equipment 101.

COPYRIGHT: (C)2003,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-198544

(P2003-198544A)

(43) 公開日 平成15年7月11日 (2003.7.11)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
H 0 4 L 9/32		G 0 6 F 15/00	3 3 0 A 5 B 0 8 5
G 0 6 F 15/00	3 3 0		3 3 0 E 5 J 1 0 4
		G 0 9 C 1/00	6 4 0 E
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 A
H 0 4 L 9/08			6 0 1 C

審査請求 未請求 請求項の数33 O L (全 22 頁) 最終頁に続く

(21) 出願番号 特願2002-301924(P2002-301924)

(22) 出願日 平成14年10月16日 (2002.10.16)

(31) 優先権主張番号 特願2001-321656(P2001-321656)

(32) 優先日 平成13年10月19日 (2001.10.19)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 山本 雅哉

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(72) 発明者 三浦 康史

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(74) 代理人 100109210

弁理士 新居 広守

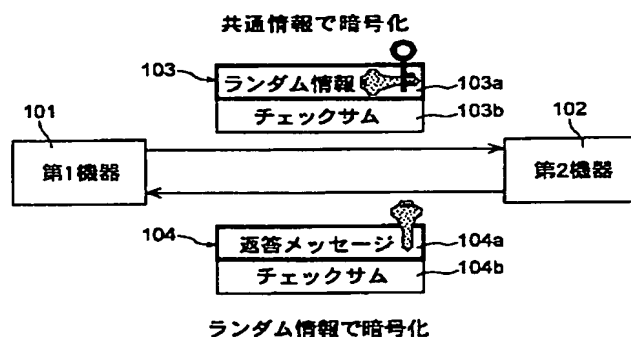
最終頁に続く

(54) 【発明の名称】 機器認証システムおよび機器認証方法

(57) 【要約】

【課題】 複数の機器間においてコンテンツのコピーや移動といった処理をする場合、それらの処理はある一定の範囲内においてのみ許可されることが想定される。全ての機器が対等の関係となる場合において、ある機器が自らと同一のグループに含まれる他の機器をセキュアに特定する機器認証システムを提供する。

【解決手段】 第1機器101より送信される送信データ103は、共通情報で暗号化されたランダム情報103a、及びチェックサム103bにより構成され、第2機器102へ送信される。前記第2機器102は、前記送信データ103を受信して、前記ランダム情報103aで暗号化した返信メッセージ104a、及びチェックサム104bで構成される返信データ104を前記第1機器101へ返信する。



【特許請求の範囲】

【請求項1】 少なくとも第1及び第2機器から構成され、前記第1及び前記第2機器が同一のグループに属するか否かを判定する機器認証システムであって、前記第1機器は、共通情報を記憶する第1共通情報記憶手段と、鍵情報を含む送信データを生成する送信データ生成手段と、生成された送信データを前記共通情報で暗号化する第1暗号化手段と、前記第1暗号化手段で得られた暗号化送信データを前記第2機器に送信する第1送信手段と、前記第2機器から送られてきた暗号化返信データを前記鍵情報で復号化する第1復号化手段と、復号化された前記返信データが一定の規則を有するか否かを判定し、一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断する認証手段とを備え、前記第2機器は、共通情報を記憶する第2共通情報記憶手段と、前記第1機器から送られてきた暗号化送信データを前記共通情報で復号化する第2復号化手段と、復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、前記送信データが一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第2暗号化手段と、前記第2暗号化手段で得られた暗号化返信データを前記第1機器に送信する第2送信手段とを備えることを特徴とする機器認証システム。

【請求項2】 前記送信データ生成手段は、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲1記載の機器認証システム。

【請求項3】 前記第1機器は、さらに、前記送信データのチェックサムを生成するチェックサム生成手段を備え、前記第1送信手段は、前記暗号化送信データとともに、前記チェックサムを前記第2機器に送信し、前記判定手段は、復号化された前記送信データのチェックサムが前記第1機器から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲1記載の機器認証システム。

【請求項4】 前記第2機器は、前記判定手段による判定により復号化された前記送信データが一定の規則を有しない場合は、前記返信データを前記第1機器に返信し

ないことを特徴とする請求の範囲1記載の機器認証システム。

【請求項5】 前記第1暗号化手段は、前記送信データと前記チェックサムとを連結して暗号化し、前記第1送信手段は、前記第1暗号化手段で得られた暗号化データを前記第2機器に送信し、前記第2復号化手段は、前記第1機器から送られてきた暗号化データを前記共通情報で復号化することによって、送信データとチェックサムとに復号し、前記判定手段は、復号化された前記送信データのチェックサムが復号化された前記チェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲1記載の機器認証システム。

【請求項6】 前記送信データ生成手段は、予め定められた固定情報を含む送信データを生成し、前記判定手段は、復号化された前記送信データに含まれる固定情報が予め定められたデータパターンであるか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲1記載の機器認証システム。

【請求項7】 前記機器認証システムには、前記第2機器が複数含まれ、前記第1送信手段は、複数の第2機器に対して前記送信データをブロードキャストすることを特徴とする請求の範囲1記載の機器認証システム。

【請求項8】 前記機器認証システムには、前記第2機器が複数含まれ、前記第1送信手段は、複数の第2機器に対して前記送信データを送信し、前記第1機器は、さらに、前記認証手段による前記複数の第2機器に対する判断に基づいて、当該第1機器と同一グループに属する第2機器の一覧を示すグループリストを生成するグループリスト生成手段と、生成されたグループリストに基づいて、第2機器と一定の通信を行うグループ通信手段とを備えることを特徴とする請求の範囲1記載の機器認証システム。

【請求項9】 前記第1機器は、さらに、前記グループリストに登録される第2機器の数が一定数を超えないように、前記送信データ生成手段、前記第1送信手段及び前記グループリスト生成手段の少なくとも1つを制御することを特徴とする請求の範囲8記載の機器認証システム。

【請求項10】 前記送信データ生成手段は、前記送信データのサイズが一定長となるように、送信データにパディングデータを含ませ、前記返信データ生成手段は、前記返信データのサイズが一定長となるように、返信データにパディングデータを含ませることを特徴とする請求の範囲1記載の機器認証

システム。

【請求項11】 前記送信データ生成手段は、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、
前記第2機器は、さらに、復号化された前記送信データに含まれる検索情報が示す物を当該第2機器が保持するか否か判定する検索情報判定手段を備え、
前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成することを特徴とする請求の範囲1記載の機器認証システム。

【請求項12】 前記送信データ生成手段は、デジタルコンテンツを特定するコンテンツIDを前記検索情報として前記送信データに含ませ、
前記返信データ生成手段は、前記送信データに含まれているコンテンツIDが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第2機器が保持する場合に、当該ライセンスを特定するライセンスIDを前記返信データに含ませることを特徴とする請求の範囲11記載の機器認証システム。

【請求項13】 前記第1機器は、さらに、
前記第2機器から送られてきた返信データに含まれるライセンスIDの一覧を示すリストを生成するリスト生成手段と、
生成されたリストに基づいて、前記第2機器とライセンスの授受のための通信を行う通信手段とを備えることを特徴とする請求の範囲12記載の機器認証システム。

【請求項14】 前記第1共通情報記憶手段及び前記第2共通情報記憶手段は、それぞれ、複数の異なる共通情報を記憶し、
前記第1暗号化手段は、前記第1共通情報記憶手段に記憶された複数の共通情報の中から選択した1つの共通情報を用いて前記送信データを暗号化し、
前記第2復号化手段は、前記第2共通情報記憶手段に記憶された複数の共通情報の中から選択した1つの共通情報を用いて前記送信データを復号化することを特徴とする請求の範囲1記載の機器認証システム。

【請求項15】 前記送信データ生成手段は、デジタルコンテンツ及びその利用形態を特定する情報を検索情報として前記送信データに含ませて前記送信データを生成し、
前記第2機器は、さらに、復号化された前記送信データに含まれる検索情報が示すデジタルコンテンツの前記利用形態による利用を可能にする権利情報であるライセンスを当該第2機器が保持するか否か判定する検索情報判定手段を備え、
前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成し、
前記第1暗号化手段は、前記第1共通情報記憶手段に記

憶された複数の共通情報の中から前記利用形態に対応した1つの共通情報を選択し、選択した共通情報を用いて前記送信データを暗号化し、

前記第2復号化手段は、前記第2共通情報記憶手段に記憶された複数の共通情報の中から前記利用形態に対応した1つの共通情報を選択し、選択した共通情報を用いて前記送信データを復号化することを特徴とする請求の範囲14記載の機器認証システム。

【請求項16】 前記第1機器は、さらに、前記第1共通情報記憶手段に記憶されている共通情報の追加及び削除を行う第1共通情報編集手段を備え、
前記第2機器は、さらに、前記第2共通情報記憶手段に記憶されている共通情報の追加及び削除を行う第2共通情報編集手段を備えることを特徴とする請求の範囲15記載の機器認証システム。

【請求項17】 少なくとも第1及び第2機器から構成され、前記第1及び前記第2機器が同一のグループに属するか否かを判定するシステムにおける機器認証方法であって、

前記第1機器及び前記第2機器は、それぞれ、共通情報を記憶する第1共通情報記憶手段及び第2共通情報記憶手段を備え、

前記機器認証方法は、

前記第1機器において、

鍵情報を含む送信データを生成する送信データ生成ステップと、

生成された送信データを前記共通情報で暗号化する第1暗号化ステップと、

前記第1暗号化ステップで得られた暗号化送信データを前記第2機器に送信する第1送信ステップと、

前記第2機器から送られてきた暗号化返信データを前記鍵情報で復号化する第1復号化ステップと、

復号化された前記返信データが一定の規則を有するか否か判定し、一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断する認証ステップとを含み、

前記第2機器において、

前記第1機器から送られてきた暗号化送信データを前記共通情報で復号化する第2復号化ステップと、

復号化された前記送信データが一定の規則を有するか否かを判定する判定ステップと、

前記送信データが一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成ステップと、

生成された返信データを前記復号化ステップで復号された送信データに含まれていた鍵情報で暗号化する第2暗号化ステップと、

前記第2暗号化ステップで得られた暗号化返信データを前記第1機器に送信する第2送信ステップとを含むこと

を特徴とする機器認証方法。

【請求項18】 前記送信データ生成ステップでは、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲17記載の機器認証方法。

【請求項19】 前記機器認証方法は、さらに、前記第1機器において、前記送信データのチェックサムを生成するチェックサム生成ステップを含み、前記第1送信ステップでは、前記暗号化送信データとともに、前記チェックサムを前記第2機器に送信し、前記判定ステップでは、復号化された前記送信データのチェックサムが前記第1機器から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲17記載の機器認証方法。

【請求項20】 前記第1暗号化ステップでは、前記送信データと前記チェックサムとを連結して暗号化し、前記第1送信ステップでは、前記第1暗号化ステップで得られた暗号化データを前記第2機器に送信し、前記第2復号化ステップでは、前記第1機器から送られてきた暗号化データを前記共通情報で復号化することによって、送信データとチェックサムとに復号し、前記判定ステップは、復号化された前記送信データのチェックサムが復号化された前記チェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲17記載の機器認証方法。

【請求項21】 前記システムには、前記第2機器が複数含まれ、前記第1送信ステップは、複数の第2機器に対して前記送信データを送信し、前記第1機器は、さらに、前記認証ステップによる前記複数の第2機器に対する判断に基づいて、当該第1機器と同一グループに属する第2機器の一覧を示すグループリストを生成するグループリスト生成ステップと、生成されたグループリストに基づいて、第2機器と一定の通信を行うグループ通信ステップとを含むことを特徴とする請求の範囲17記載の機器認証方法。

【請求項22】 前記送信データ生成ステップでは、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、前記機器認証方法は、さらに、前記第2機器において、復号化された前記送信データに含まれる検索情報が示す物を当該第2機器が保持するか否かを判定する検索情報判定ステップを含み、前記返信データ生成ステップでは、前記検索情報判定ステップによる判定結果を前記返信データに含ませて前記返信データを生成することを特徴とする請求の範囲17記載の機器認証方法。

【請求項23】 前記送信データ生成ステップでは、デジタルコンテンツを特定するコンテンツIDを前記検索情報として前記送信データに含ませ、

前記返信データ生成ステップでは、前記送信データに含まれているコンテンツIDが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第2機器が保持する場合に、当該ライセンスを特定するライセンスIDを前記返信データに含ませることを特徴とする請求の範囲22記載の機器認証方法。

【請求項24】 前記第1共通情報記憶手段及び前記第2共通情報記憶手段は、それぞれ、複数の異なる共通情報を記憶し、

前記第1暗号化ステップでは、前記第1共通情報記憶手段に記憶された複数の共通情報の中から選択した1つの共通情報を用いて前記送信データを暗号化し、前記第2復号化ステップでは、前記第2共通情報記憶手段に記憶された複数の共通情報の中から選択した1つの共通情報を用いて前記送信データを復号化することを特徴とする請求の範囲17記載の機器認証方法。

【請求項25】 相手装置と相互に認証し合うことによって、相手装置と自装置とが同一グループに属するか否かを判定する通信装置であって、

相手装置を認証するための認証部と、相手装置から認証してもらうための被認証部とを備え、前記認証部は、共通情報を記憶する共通情報記憶手段と、鍵情報を含む送信データを生成する送信データ生成手段と、

生成された送信データを前記共通情報で暗号化する第1暗号化手段と、

前記第1暗号化手段で得られた暗号化送信データを前記相手装置に送信する第1送信手段と、

前記相手装置から送られてきた暗号化返信データを前記鍵情報で復号化する第1復号化手段と、

復号化された前記返信データが一定の規則を有するか否かを判定し、一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断する認証手段とを有し、

前記被認証部は、

前記相手装置から送られてきた暗号化送信データを前記共通情報で復号化する第2復号化手段と、

復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、

前記送信データが一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第2暗号化手段と、

前記第2暗号化手段で得られた暗号化返信データを前記

相手装置に送信する第2送信手段とを有することを特徴とする通信装置。

【請求項26】 前記送信データ生成手段は、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲25記載の通信装置。

【請求項27】 前記相手装置は、さらに、前記送信データのチェックサムを生成するチェックサム生成手段を備え、

前記第1送信手段は、前記暗号化送信データとともに、前記チェックサムを前記相手装置に送信し、

前記判定手段は、復号化された前記送信データのチェックサムが前記相手装置から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲25記載の通信装置。

【請求項28】 相手装置と相互に認証し合うことによって、相手装置と自装置とが同一グループに属するか否かを判定する通信装置のためのプログラムであって、相手装置を認証するための認証ステップと、相手装置から認証してもらうための被認証ステップとを含み、

前記認証ステップは、鍵情報を含む送信データを生成する送信データ生成ステップと、

生成された送信データを予め記憶している共通情報で暗号化する第1暗号化ステップと、

前記第1暗号化ステップで得られた暗号化送信データを前記相手装置に送信する第1送信ステップと、

前記相手装置から送られてきた暗号化返信データを前記鍵情報で復号化する第1復号化ステップと、

復号化された前記返信データが一定の規則を有するか否かを判定し、一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断する認証ステップとを含み、

前記被認証ステップは、

前記相手装置から送られてきた暗号化送信データを前記共通情報で復号化する第2復号化ステップと、

復号化された前記送信データが一定の規則を有するか否かを判定する判定ステップと、

前記送信データが一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成ステップと、

生成された返信データを前記復号化ステップで復号された送信データに含まれていた鍵情報で暗号化する第2暗号化ステップと、

前記第2暗号化ステップで得られた暗号化返信データを前記相手装置に送信する第2送信ステップとを含むことを特徴とするプログラム。

【請求項29】 前記送信データ生成ステップは、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲28記載のプログラム。

【請求項30】 前記プログラムは、さらに、前記送信データのチェックサムを生成するチェックサム生成ステップを含み、

前記第1送信ステップは、前記暗号化送信データとともに、前記チェックサムを前記相手装置に送信し、

前記判定ステップは、復号化された前記送信データのチェックサムが前記相手装置から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲28記載のプログラム。

【請求項31】 少なくとも第1及び第2機器から構成され、前記第1及び前記第2機器が同一のグループに属するか否かを判定する機器認証システムに用いられる認証データが記録されたコンピュータ読み取り可能な記録媒体であって、

前記認証データには、

鍵情報を含む送信データが共通情報で暗号化された暗号化送信データと、

前記送信データのチェックサムとが含まれ、

前記認証データは、前記第1機器から前記第2機器に送信されるデータであり、

前記鍵情報は、前記第1機器が前記第2機器と同一のグループに属すると前記第2機器が判断した場合に、前記第2機器が前記第1機器に返信する返信データの暗号化に用いられ、

前記共通情報は、同一のグループに属する機器が予め保持する情報であることを特徴とする記録媒体。

【請求項32】 前記鍵情報は、前記第1機器で生成された乱数であることを特徴とする請求の範囲31記載の記録媒体。

【請求項33】 前記送信データには、デジタルコンテンツを特定するコンテンツIDが含まれ、

前記返信データには、前記送信データに含まれているコンテンツIDが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを特定するライセンスIDが含まれることを特徴とする請求の範囲31記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、同一ネットワークにおいて各機器が他の機器の認証を行う場合に必要となる機器認証システムに関するものであり、特に、複数の端末機器間における機器認証システムに関するものである。

【0002】

【従来の技術】近年、音楽や映像、ゲーム等デジタルコ

コンテンツはインターネットやデジタル放送及び、パッケージメディアによる流通により容易に取得が可能となってきた。そうしたデジタルコンテンツ及びその権利を複数の端末間においてコピーや移動を行う際には、無制限な範囲での移動は許されず、ある一定範囲内でのコピーや移動のみが許されるのが一般的である。

【0003】一般的には同一ユーザが所有する複数の端末間においてのみコピーや移動が許されると考えられている。このような一定範囲内でのコピーや移動を実現するためには、当該端末群によってコピーや移動が相互に可能なグループを形成する必要がある。

【0004】従来、このようなグループの判定はサーバ（グループ判定端末）が行うことが想定されている。以下、サーバにおけるグループ判定について簡単に説明する。

【0005】従来のグループ判定システムはグループの判定を行うサーバとネットワークとにより通信可能に接続される被管理端末群からなる。サーバはグループごとに該当する端末のグループリストを保持している。グループリストとは例えばグループ識別子と端末識別子とを関連付ける情報である。

【0006】以上の構成のグループ判定システムでは、以下のようにグループの判定が行われる。まず、被管理端末は自らが属するグループの端末リストを取得する場合、サーバに端末リスト要求データを送信する。前記端末リスト要求データには、例えば自らの端末識別子、グループ識別子といったものが含まれる。サーバは端末リスト要求データに含まれる情報に従って該当するグループリストを前記被管理端末に送信する。以上の処理を経て被管理端末は自らの属するグループ情報を取得することによりグループの判定を実現している。

【0007】例えば、従来のメンバー識別方法では、ホスト端末が全メンバー及びホスト端末固有のネットワークアドレスをデータとしたパケットを同報送信し、メンバー端末は、受信パケットを解析し自分の名前が入ったパケットからの情報を取り出して識別し、各メンバー名と各メンバー端末固有のネットワークアドレスをデータとするパケットをホスト端末へ送信し、ホスト端末は、受信パケットを解析し、同一グループに属するメンバーの名前があった場合には、そのパケットに含まれる情報を取得し、メンバー名と端末アドレスとを対応させ、対応データをセーブしてグループの識別を行っている（例えば、特許文献1参照。）。

【0008】

【特許文献1】特開平10-23028号公報

【0009】

【発明が解決しようとする課題】まず、従来のグループ判定方法が抱えている問題点について説明すると、従来のグループ判定方法においては、サーバ端末（グループ判定端末）と被管理端末とは親子関係が生じ、サーバ

端末と被管理端末とで異なる機能を持つ必要がある。

【0010】次に、従来の判定方法を一般的なユーザが使用する家電製品等に適用することを考える。従来の判定方法を適用するにはユーザは自らの保持する家電製品の親子関係を把握し、かつ購入時にどのように親子関係を設定するかも想定しながら購入する必要がある。なぜならグループ判定においてサーバ端末は必須であり、またサーバ端末と被管理端末とは機能や価格等が異なることが想定されるためである。

【0011】本来、家電製品のように随時端末が追加されていき、様々な利用の仕方が想定される端末は、端末間の関係が対等であるべきと考えられる。つまり、従来は全ての端末が対等の関係となる場合にグループを構成するための方法は知られていない。

【0012】そこで、前記課題に鑑み、本発明に係る機器認証システムにおいては、各端末機器も対等の関係になる場合において同一グループに属する機器の特定を可能とする。

【0013】また、本発明に係る機器認証システムは、端末機器が認証処理、コンテンツ送受信処理等の端末に負荷の大きい処理を行う前に、安全に同一グループに属する端末のグループリストを取得することを目的とする。そして、本発明に係る機器認証システムは、前記グループリストを利用することにより、送信データの送信先となる機器を決定して、コンテンツの取得が不可能な端末に対しては通信を行わずに、通信経路の効率的な利用等を可能とすることを目的とする。

【0014】さらに、本発明は、将来のコンテンツの有料ネットワーク配信の普及に対応した機器認証システムを提供することをも目的とする。

【0015】

【課題を解決するための手段】前記目的を達成するために、本発明に係る機器認証システムでは、少なくとも第1及び第2機器から構成され、前記第1及び前記第2機器が同一のグループに属するか否かを判定する機器認証システムであって、前記第1機器は、共通情報を記憶する第1共通情報記憶手段と、鍵情報を含む送信データを生成する送信データ生成手段と、生成された送信データを前記共通情報で暗号化する第1暗号化手段と、前記第1暗号化手段で得られた暗号化送信データを前記第2機器に送信する第1送信手段と、前記第2機器から送られてきた暗号化返信データを前記鍵情報で復号化する第1復号化手段と、復号化された前記返信データが一定の規則を有するか否かを判定し、一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断する認証手段とを備え、前記第2機器は、共通情報を記憶する第2共通情報記憶手段と、前記第1機器から送られてきた暗号化送信データを前記共通情報で復号化する第2復号化手段と、復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、前記送信

データが一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第2暗号化手段と、前記第2暗号化手段で得られた暗号化返信データを前記第1機器に送信する第2送信手段とを備えることを特徴とする。

【0016】また、前記目的を達成するために、本発明は、前記送信データ生成手段は、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする。さらに、本発明は、前記第1機器は、さらに、前記送信データのチェックサムを生成するチェックサム生成手段を備え、前記第1送信手段は、前記暗号化送信データとともに、前記チェックサムを前記第2機器に送信し、前記判定手段は、復号化された前記送信データのチェックサムが前記第1機器から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする機器認証システムとなる。

【0017】さらに、前記目的を達成するために、本発明に係る機器認証システムでは、前記機器認証システムには、前記第2機器が複数含まれ、前記第1送信手段は、複数の第2機器に対して前記送信データをブロードキャストする。

【0018】そして、前記目的を達成するために、本発明に係る機器認証システムは、前記送信データ生成手段は、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、前記第2機器は、さらに、復号化された前記送信データに含まれる検索情報が示す物を当該第2機器が保持するか否かを判定する検索情報判定手段を備え、前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成することを特徴とする。

【0019】前記目的を達成するために、本発明に係る機器認証システムは、前記送信データ生成手段は、デジタルコンテンツを特定するコンテンツIDを前記検索情報として前記送信データに含ませ、前記返信データ生成手段は、前記送信データに含まれているコンテンツIDが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第2機器が保持する場合に、当該ライセンスを特定するライセンスIDを前記返信データに含ませることを特徴とする。

【0020】尚、本発明は、上述のような機器認証システムとして実現できるのみではなく、この機器認証システムが備える手段をステップとする機器認証方法、及び当該手段を装置上で実現する通信装置としても実現することができる。

【0021】また、前記機器認証方法をコンピュータ等

で実現させるプログラムとして実現したり、当該プログラムをCD-ROM等の記録媒体や通信ネットワーク等の伝送媒体を介して流通させることができるのは言うまでもない。

【0022】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態について説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定するものではない。以下、本発明に係る実施の形態について図面を用いて説明する。

【0023】ここで詳細の説明に先立ち、本発明におけるグループの定義を行う。互いにコンテンツ又はコンテンツに対する権利をコピーや移動といった処理が相互に可能な端末が存在する場合に、それらの端末群は論理的にグルーピングが可能である。そしてグルーピングした端末群の属する単位を認可範囲(Authorized Domain)とし、以下、簡単のためグループと呼ぶ。

【0024】(実施の形態1)図1は、本発明の実施の形態1に係る機器認証システムを説明する概略図である。図1において、第1機器101と第2機器102とは有線又は無線の伝送路を介してデータ通信可能に接続される。ここで、第1機器101は他の機器が自らと同一グループに属するか判定する機器に相当し、第2機器102は、自らのグループに属するか否かを尋ねてきた機器に対して、応答する機器に相当する。また、本実施の形態1においては、端末機器は第1機器101と第2機器102とで説明を行うが、ブロードキャストの到達範囲内における全ての端末機器に対して同様の方法により機器認証を行うことができる。

【0025】第1機器101は、例えば、ユーザの利用する機器であり、PC、携帯電話、セットトップボックス等である。この第1機器101は、グループ化を行いグループリストを作成する機器であり、グループ化を行うために送信データ103を作成して、この送信データ103を暗号化して第2機器102へ送信する。

【0026】第2機器102は、前記第1機器101と同様に、例えばPC、携帯電話、セットトップボックス等の端末機であり、ブロードキャスト到達範囲内にあり、第1機器101より送信される送信データ103を受信して返信データ104を暗号化して第1機器101へ返送する。

【0027】送信データ103は、ランダム情報103aとチェックサム103bとを備えており、このランダム情報103aは、第1機器101で生成されるランダムなバイト列であるパスワード等の共通情報により暗号化されている。また、チェックサム103bは、送信前にランダム情報103a等のデータを分割し、それぞれのブロック内のデータを数値とみなして合計した情報であり、本実施の形態1においては、暗号化はされずに送

信される。尚、このチェックサム103bを共通情報等により暗号化して送信することも可能である。

【0028】返信データ104は、第1機器101より投げかけられた情報に返信するためのデータであり、返信メッセージ104aとチェックサム104bとを含む。返信メッセージ104aには、例えば同一グループであることが記載され、受信したランダム情報103aを用いて暗号化される。また、チェックサム104bは、前記チェックサム103bと同様に、送信前に返信メッセージ104a等のデータを分割し、それぞれのブロック内のデータを数値とみなして合計した情報であり、本実施の形態1においては、暗号化はされずに返送される。

【0029】図2を用いて第1機器101が他の機器に対して自らと同一グループに属するか否かを判定する場合の流れを説明する。尚、実施の形態1では同一グループに属するか否かは共通情報Aを保持しているか否かに起因している。即ち、本発明の方法でグループ判定処理を行う場合、同一グループに属する機器は共通情報Aを保持しておくことを前提としている。

【0030】図2は、本実施の形態1に係る複数の機器とグループとの関係を示す図である。この機器認証システムは、第1機器101と、第2機器102と、第6機器201と、第7機器202とが存在し、本実施の形態1において、第1機器101は、自らと同じグループである他の機器をフィルタリングする機器に該当し、ブロードキャストにより他の機器に対して自らと同一グループに属するか否かを判定する。図2において、第1機器101と、第2機器102とは同一グループであるドメイン1 (Authorized Domain1) に属し、第7機器202は別のグループとなるドメイン2 (Authorized Domain2) に属するものとする。

【0031】第1機器101は、PC等の端末機であり、通信可能なブロードキャスト到達範囲である第2機器102及び第7機器202に共通情報Aで暗号化した送信データをブロードキャストする。ここで通信可能な範囲には、例えば家庭内のホームネットワーク等が含まれる。

【0032】第2機器102は、共通情報Aを保持しており、この共通情報Aにより暗号化された送信データを復号化することができ、通信エラーを考えなければ正しい返信データを第1機器101へ返信することができる。また、第1機器101は、この返信データを受信し、所定の処理を行うことにより、第2機器102が同一グループに属すると判断する。

【0033】第7機器202は、保持している共通情報Cが共通情報Aと異なるため、共通情報Aにより暗号化された送信データの受信後、所定の処理を行うと第7機器202に備えられているチェックサム判定部においてチェックサム不一致となり返信データを返さない。ま

た、偶然、第7機器202のチェックサム判定においてチェックサムが一致したとしても、第1機器101のチェックサム判定によりチェックサム不一致となり、同一グループの機器リストとして第7機器202はフィルタリングされない。尚、ブロードキャスト到達範囲外にある第6機器201は、送信データが到達しないため同一グループと判定されることはない。

【0034】以上の判定方法により、第1機器101は、共通情報Aを送信することなく同一グループに属する機器のグループリストを作成することができる。このグループリストに含まれる機器は、少なくとも同一の共通情報Aを保持することが保証され、即ち同一グループに属することが保証される。

【0035】以下、第1機器101及び第2機器102について順番に、それぞれの詳細な構成について説明する。図3は、本実施の形態1に係る第1機器101の詳細な構成を示すブロック図である。第1機器101は、ブロードキャストを行い同一グループに属する端末機器のグループリスト構成を行う端末であり、ランダムなバイト列を生成するランダム情報生成部301と、暗号／復号部302と、パスワード等の共通情報を記憶している共通情報記憶部303と、チェックサム生成部304と、機器間通信部305と、チェックサム判定部306を備えている。尚、前記チェックサムとは送信前のデータを分割し、それぞれのブロック内のデータを数値とみなして合計を取ったものである。

【0036】まず第1機器101が第2機器102へ送信データT-Data1を送信する場合のデータの流について説明する。ランダム情報生成部301は、ランダムなバイト列を生成し、このバイト列をセッション鍵情報、パディングデータ等のランダム情報R1として用いると共に、このランダム情報R1をタイムアウト時間まで保持する。このタイムアウト時間とは、ランダム情報R1を生成してから他の機器からの返信を待つ最後の時間まで値を示し、機器においてユーザ或いは機器メーカーが設定する。また、ランダム情報生成部301は、ランダム情報R1をチェックサム生成部304及び暗号／復号部302へ送信する。

【0037】暗号／復号部302は、共通情報Aを用いてランダム情報R1の暗号化を行い、この暗号化された暗号化情報E1を機器間通信部305へ送信する。共通情報記憶部303は、共通情報Aを記憶するハードディスク等を有しており、この共通情報Aは、通常ユーザ自らが入力するのではなくサーバ側が管理しており、入会時や購入時においてサーバ側より共通情報記憶部303へ入力される情報である。

【0038】チェックサム生成部304は、受信した前記ランダム情報R1のチェックサム対象部のデータのブロック内のデータの数値の合計をCS1として生成し、このCS1を機器間通信部305へ送信する。そして、

機器間通信部305は、受信したチェックサムCS1と暗号化情報E1とにより送信データT-D a t a 1の packets を構築して、これを送信データT-D a t a 1として第2機器102側へ送信する。

【0039】一方、第1機器101が第2機器102から返送された返信データA-D a t a 2を受信する場合のデータの流れについて説明する。まず、機器間通信部305は、他の機器である第2機器102とデータの送受信を行い、受信した返信データA-D a t a 2のうち暗号化情報E2を復号化するため暗号／復号部302へ送信すると共に、返信データA-D a t a 2に付与されているCS3をチェックサム判定部306へ送信する。

【0040】暗号／復号部302は、暗号化情報E2の復号化をランダム情報R1を用いることにより行い、復号化された復号済み応答データDA2をチェックサム生成部304へ送信する。チェックサム生成部304は、受信した前記復号済み応答データDA2のチェックサム対象部のデータのブロック内のデータの数値の合計をCS4として生成し、このCS4をチェックサム判定部306へ送信する。

【0041】チェックサム判定部306は、同一グループに属する機器を記憶する記憶部であるグループリストを備えており、前記CS3と前記CS4との比較を行い、判定の結果、一致する場合には第2機器102を同一グループに属する機器としてグループリストへ追加する。また、判定の結果チェックサムが一致しない場合には、第2機器102を同一グループに属さない機器と判断してグループリストへの追加を行わない。尚、前記復号済み応答データDA2は暗号／復号部302が送信するとしたが、チェックサム判定部306が取得要求を送信するとしてもよい。

【0042】図4は、本実施の形態1に係る第2機器102の詳細な構成を示すブロック図である。第2機器102は、前記第1機器101と同様な暗号／復号部402と、共通情報記憶部403と、チェックサム生成部404と、機器間通信部405と、チェックサム判定部406との構成に加えて、さらに、同一グループに属する等の情報を含む応答データADを生成する応答データ生成部407を備えている。尚、第1装置101に備えられるランダム情報生成部301は備えられていない。

【0043】第2機器102が第1機器101から受信する送信データT-D a t a 1の流れについて説明すると、機器間通信部405は、送信データT-D a t a 1を受信し、この送信データT-D a t a 1のうち暗号化情報E1を暗号／復号部402へ送信すると共に、CS1をチェックサム判定部406へ送信する。

【0044】暗号／復号部402は、共通情報記憶部403に記憶されている共通情報Aにより前記暗号化情報E1の復号化を行い、復号化された復号済みデータDR1をチェックサム生成部404へ送信する。

【0045】チェックサム生成部404は、前記復号化済みデータDR1のチェックサム対象部のデータのブロック内のデータの数値の合計をCS2として生成し、このCS2をチェックサム判定部406へ送る。チェックサム判定部406においては、前記CS1と前記CS2との比較を行い、判定の結果一致していれば、同一グループの属する機器からの送信データT-D a t a 1として応答データ生成部407へ応答データADの作成を指示する。

【0046】応答データ生成部407は、前記指示により、同一グループに属する等のデータを含んだ応答データADの生成を行い、この応答データADを暗号／復号部402とチェックサム生成部404とへ送信する。暗号／復号部402は、応答データADを暗号化情報E1に含まれるランダム情報R1で暗号化して暗号化データE2として機器間通信部405へ送る。また、チェックサム生成部404は、応答データADのチェックサム対象部のデータのブロック内のデータの数値の合計をCS3として生成して機器間通信部405へ送る。尚、前記暗号化においてはランダム情報R1を用いて暗号化するのではなく、共通情報Aを用いて暗号化することもできる。

【0047】機器間通信部405は、前記暗号化データE2と前記CS3とを含んだパケットデータである返信データA-D a t a 2を生成して第1機器101側へ返送し、一連の機器認証システムにおけるデータ処理を終了する。

【0048】図5は、本実施の形態1に係る送信データT-D a t a 1のデータ構成を示す図である。尚、この図5は、本実施の形態1の説明のために例示するものである。

【0049】送信データT-D a t a 1は、第1機器101より他の機器へ送信され、他の機器が第1機器101と同一グループに属するか否かの返答要求メッセージであり、メッセージヘッダ501、クライアントID502、ランダム情報503、パディングデータ504、チェックサム505より構成されている。

【0050】メッセージヘッダ501は、同一グループに属するか否かのメッセージ等を含み、送信データT-D a t a 1の先頭領域に位置しており、暗号化されずに送信されるデータである。クライアントID502は、メッセージ送信元である第1機器101のクライアントIDが保持されている。

【0051】ランダム情報503は、ランダムなバイト列で構成され、返信データを暗号化する際に用いられるセッション鍵等の情報を含む。このセッション鍵の情報は、タイムアウト時間まで第1機器101側において保持され、返信データの暗号化部を復号化する際に用いられる情報である。

【0052】パディングデータ504は、予備的なデー

タであり、例えば、暗号アルゴリズムがAESであり、送信データT-D a t a 1のデータ長が暗号化単位の8バイトの倍数となっていない際に送信データT-D a t a 1が8バイトの倍数となるように付与されるデータである。そして、共通情報により暗号化され、暗号強度を増すためにパディングデータ504で暗号化対象データ部EDを長くしてもよい。尚、パディングデータ504の代わりに2バイト程度のリザーブフィールドを設けることも考えられる。

【0053】チェックサム505は、クライアントID502とランダム情報503とパディングデータ504とから成るチェックサム対象部CTのデータのブロック内のデータの数値の合計を保持している。また、CRC32のようなチェックサム・アルゴリズムの代わりにハッシュ関数を用いてもよく、例えばSHA-1やMD5としてもよい。

【0054】暗号化対象データEDは、クライアントID502、ランダム情報503、及びパディングデータ504により構成され、少なくともランダム情報503を含むものとする。また、暗号化対象データEDには第1機器101をネットワーク上で一意に識別する機器識別情報を含んでもよい。ここで機器識別情報は、具体的には自らのIPアドレス、機器の識別子であるクライアントID502等となる。尚、返信データを返送する場合等にIPアドレスが必要であれば、送信データT-D a t a 1にIPアドレスを含めることも可能である。

【0055】図6を用いて返信データA-D a t a 2の内容について説明する。図6は、本実施の形態1に係る返信データA-D a t a 2のデータ構成を示す図である。尚、この図6は、本実施の形態1の説明のために例示するものであり、本発明はこの構成に限定されるものではない。

【0056】返信データA-D a t a 2は、第1機器101より送信される返答要求メッセージである送信データT-D a t a 1に対する返信である。この返信データA-D a t a 2は、メッセージヘッダ601、クライアントID602、共通情報603、パディングデータ604、及びチェックサム605より構成される。

【0057】メッセージヘッダ601は、同一グループに属するか否かのメッセージ等であり、クライアントID602は返信データA-D a t a 2の送信元となる第2機器102のクライアントIDである。共通情報603は、第1機器101と第2機器102とが共通して有しているパスワード等の共通情報であり、本実施の形態1においては共通情報Aである。

【0058】パディングデータ604は、予備的なデータであり、暗号強度を増すためにパディングデータ604で応答データADを長くすることも可能である。チェックサム605は、クライアントID602と共通情報603とパディングデータ604とから成るチェックサ

ム対象部CTのデータのブロック内のデータの数値の合計である。

【0059】応答データADは、クライアントID602と共通情報603とパディングデータ604とより成り、第2機器102が共通情報Aを保持していることを確認するために共通情報603を含んでいる。この応答データADは、前記ランダム情報503に含まれるセッション鍵等を用いて暗号化されてから返信される。

【0060】また、応答データADは、少なくとも第2機器102をネットワーク上で一意に識別する機器識別情報を含む。ここで機器識別情報は、自らのIPアドレス、機器の識別子であるクライアントID602等を想定する。尚、応答データADは少なくとも機器識別情報を含むとしたが、機器間において通信を行う場合に付与される通信プロトコルに応じたメッセージヘッダに機器識別情報相当（例えば自らのIPアドレス）の情報が含まれる場合はこの限りではない。

【0061】本発明の機器認証システムを用いる準備としての共通情報の機器への設定の仕方について以下に例を示す。図7は、本実施の形態1におけるユーザインターフェイスの画面を示す図である。グループの設定範囲は、一般に同一ユーザが所有する複数の機器群を想定している。グループの設定を行うユーザは共通情報を何らかの方法で入手し、同一グループに属する機器に図7

(a)に示すようなUIで入力処理を行う。尚、機器に共通情報を設定するユーザを限定するためパスワード等を設けてもよい。ユーザの共通情報の入手方法については、図7(b)に示すように、例えば、ある機器の共通情報である「zeppetstore」を表示させ、それを同一グループに設定する他の機器に入力する。また、共通情報は機器メーカー、販売店等から葉書やeメール等により入手してもよいし、ユーザが考えて同一グループに設定する他の機器に設定してもよい。

【0062】また、共通情報はユーザには提示せず、機器メーカー、販売店等がユーザの要求、或いはメーカー、販売店のポリシーにより出荷時、販売時に設定してもよい。そして、ICカードに共通情報を記憶し、各機器が挿入したICカードの情報を読み込むことにより共通情報を設定するとしてもよい。尚、ICカードの入手方法は共通情報の入手で上述したようにあらゆる方法を想定する。また、ICカードの代わりに記憶媒体、或いはSDカード等のデータをセキュアに管理できる記憶媒体を用いてもよい。

【0063】尚、通常は、ユーザが共通情報等を自ら入力するのではなく、サーバ側が管理して、サーバ側よりグループ入会時、PC購入時等において各端末機器へ伝送路を介して自動的に入力される。このため、ユーザが共通情報を知ることにより、同一グループに属する対象となる端末機器が故意に広がってしまう可能性を防止する。

【0064】次に、第1機器101が作成するグループリストの情報項目についての内容の一例を説明する。図8は、本実施の形態1における第1機器101が作成するグループリストの情報項目を示す図である。図8

(a)においてグループを識別するグループID(801a)の項目があり、グループID(801a)に対してグループに属する機器の識別情報が記述される。機器の識別情報としてはデバイスID(802a、803a)等を記述する。また、グループID(801a)に対応してグループの範囲内で許される可能な処理について記述してもよい。この可能な処理としては、図8

(a)においては「コピー」であり、他には再生、移動等も考えられる。

【0065】図8(b)においても同様であり、グループを識別するグループID(811b)の項目があり、グループID(811b)に対してグループに属する機器の識別情報としてデバイスID(812b、813b)等を記述する。また、図8(b)において、範囲内で許される可能な処理は「移動」である。

【0066】また、機器ごとに複数のグループに属していてもよく、その場合、機器は複数のグループに対応する複数の共通情報を保持し、処理により図8(a)又は(b)のように複数のグループIDに対するグループリストを保持することも可能とする。

【0067】グループリストの生成が完了すると、グループリストに含まれる機器と通信を行い、同一グループ内で許可されている処理等を行う。以降の認証処理、コンテンツ取得処理等は一般的な方法でセキュアに行う。尚、グループリストはコンテンツのコピーや移動の処理の度に生成し、処理終了後、即時削除することにすれば、処理の度に常に最新のグループ情報を取得することが可能となる。

【0068】本実施の形態1においては、ユーザメリットとなるグループ設定、及びグループ判定方法について説明するが、コンテンツホルダーの立場からはグループの定義範囲をあまり広げたくない場合も想定される。そのような場合はグループリストに記述できる機器識別情報の最大値を設定し、他の端末からの返信データによりグループリストを作る際に、最大値に達したらグループリストの生成処理を強制的に終了するようにしてもよい。以上の処理を行い、常に機器は正常に動作し、かつネットワーク構成が変わらないことを前提とすると、ユーザは最大値+ α くらいの機器しか同一グループに設定できなくなる。少なくともグループ内の機器を無限に増やすことを防ぐことが可能となる。

【0069】また、同一グループの設定については上述したが、共通情報の新規入力や削除の処理により同一グループ内に属する機器を柔軟かつ容易に設定可能である。

【0070】次に、以上のように構成された本実施の形

態1に係る機器認証システムの動作について説明する。

図9は、本実施の形態1に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。尚、本実施の形態1においては、第1機器101が、第2機器102と同一グループに属するか否かを判定する場合の説明を行うが、同様の機器認証システムを用いることにより、ブロードキャスト等において複数の端末機器間においても同一グループ判定を行うことが可能である。また、機器認証システムの動作の説明においては、図3及び図4の符号を参照するものとする。

【0071】最初に、第1機器101を構成するランダム情報生成部301は、ランダム情報R1を生成し、同じく第1機器101を構成する暗号/復号部302、及びチェックサム生成部304に送信する(ステップ901)。尚、本実施の形態1においては、ランダム情報生成部301は、タイムアウト時間まではランダム情報R1を保持しておかなければならない。また、タイムアウト時間前であってもユーザによる終了指示によりランダム情報R1をランダム情報生成部301から削除してもよい。また、ランダム情報R1は何バイトかのランダムなバイト列であり、バイト数については暗号/復号処理に用いる暗号アルゴリズム等に依存する。

【0072】続いて、暗号/復号部302は、ランダム情報生成部301よりランダム情報R1を受信すると共通情報記憶部303に共通情報取得要求を送信し、共通情報記憶部303より共通情報Aを受信する。次に、暗号/復号部302は、少なくともランダム情報R1を含む暗号化対象データEDを共通情報Aを鍵として暗号化を行い、暗号化情報E1を生成し、機器間通信部305に送信する(ステップ902)。ここで暗号のアルゴリズムとしては一般的に暗号強度が使用に耐えうるものを採用し、例えばDES、TripleDES、AES等を想定する。尚、以下では暗号/復号部302及び図4における暗号/復号部402は1つの同じ暗号アルゴリズムを保持することとして記述するが、複数の暗号アルゴリズムを保持してもよい。但し、複数暗号アルゴリズムを保持する場合は暗号アルゴリズム識別子が必要となるし、第1機器101及び第2機器102が前記暗号アルゴリズム識別子に対応する同じ暗号アルゴリズムを保持しておかなければならない。

【0073】次に、チェックサム生成部304は、少なくともランダム情報R1を含む前記暗号化対象データEDに対するCS1を生成し、機器間通信部305に送信する(ステップ903)。

【0074】機器間通信部305は、暗号化情報E1と前記CS1との両者を受信すると少なくとも前記暗号化情報E1と前記CS1とを含み、通信プロトコルに応じたメッセージヘッダ等を付した送信データT-Dat a 1を他の機器に対して送信する(ステップ904)。

【0075】次に、第2機器102に備えられる機器間

通信部405は、第1機器101より前記送信データT-Data1を受信し、送信データT-Data1より前記暗号化情報E1と前記CS1とを抽出する(ステップ905)。

【0076】次に、機器間通信部405は、暗号化情報E1を同じく第2機器102を構成する暗号/復号部402へ、CS1を同じく第2機器102を構成するチェックサム判定部406へ送信する。

【0077】暗号/復号部402は、暗号化情報E1を受信すると、共通情報記憶部403に共通情報取得要求を送信し、共通情報記憶部403より共通情報Aを受信する。暗号/復号部402は暗号化情報E1を共通情報Aを鍵として復号化を行い、復号された暗号化情報(以下、復号済み暗号化対象データと呼ぶ)DR1を取得し、チェックサム生成部404に送信する(ステップ906)。また、暗号/復号部402は応答データ生成部407から応答データADが送信されてくるまで、取得した復号済み暗号化対象データDR1を保持する。

【0078】続いて、チェックサム生成部404は、受信した復号済み暗号化対象データDR1に対するCS2を生成し、チェックサム判定部406へ送信する(ステップ907)。チェックサム判定部406は受信したCS1とCS2との比較処理を行う(ステップ908)。

【0079】そして、チェックサム判定部406は、比較処理の結果、CS1=CS2となった場合はチェックサム一致の制御コードを、CS1≠CS2の場合はチェックサム不一致の制御コードを応答データ生成部407に送信する。

【0080】応答データ生成部407は、チェックサム不一致の制御コードを受信した場合、応答データは生成しない(ステップ909)。尚、応答データADを意味のないバイト列であるパディングデータ等で埋めたり、エラーコードを記述するとしてもよいが、本実施の形態1ではチェックサム不一致の場合、応答データADを生成しないこととして説明を進める。また、チェックサム不一致の場合、チェックサム判定部406が応答データ生成部407に制御コードを送信しないとしてもよい。

【0081】応答データ生成部407は、制御コードを受信し、制御コードに応じた応答データADを生成し、暗号/復号部402及びチェックサム生成部404に送信する(ステップ910)。

【0082】尚、正しい応答データADを第1機器101に返信した機器は少なくとも同一グループに属しているという判断を行うため、チェックサムの不一致が通信エラーに起因するものであっても同様の判断を行ってよい。

【0083】続いて、暗号/復号部402は、受信した応答データADを保持している復号済み暗号化対象データDR1からランダム情報R1を抽出し、セッション鍵等のランダム情報R1を鍵として暗号化を行い、暗号化

情報E2を生成し、機器間通信部405に送信する(ステップ911)。また、チェックサム生成部404は受信した応答データADに対するCS3を生成し、機器間通信部405に送信する(ステップ912)。機器間通信部405は暗号化情報E2とCS3との両者を受信すると、少なくとも暗号化情報E2とCS3とを含み、通信プロトコルに応じたメッセージヘッダ等を付した返信データA-Data2を第1機器101に対して送信する(ステップ913)。

【0084】次に、第1機器101に備えられる機器間通信部305は、第2機器102より返信データA-Data2を受信し、暗号化情報E2とCS3とを抽出する(ステップ914)。次に、機器間通信部305は、暗号化情報E2を暗号/復号部302へ、CS3をチェックサム判定部306へ送信する。

【0085】暗号/復号部302は、機器間通信部305より暗号化情報E2を受信するとランダム情報生成部301にランダム情報取得要求を送信し、ランダム情報生成部301よりランダム情報R1を受信する。暗号/復号部302は、受信した暗号化情報E2を同じく保持していたランダム情報R1を鍵として復号化を行い、復号された暗号化情報(以下、復号済み応答データと呼ぶ)DA2を取得し、チェックサム生成部304及びチェックサム判定部306に送信する(ステップ915)。尚、チェックサム判定部306に送る際に復号済み応答データDA2より機器識別情報を抽出して送信してもよい。

【0086】続いて、チェックサム生成部304は、受信した復号済み応答データDA2に対するCS4を生成し、チェックサム判定部306へ送信する(ステップ916)。チェックサム判定部306は受信したCS3とCS4との比較処理を行う(ステップ917)。

【0087】まず、比較処理の結果、CS3=CS4となった場合は応答データADを送信してきた第2機器102が同一グループに属すると判断し、第2機器102が同一グループに属する機器としてリストに追加する(ステップ919)。一方、CS3≠CS4の場合は同一グループに属しないと判断し処理を終了する(ステップ918)。また、第2機器102のチェックサム不一致と同様の理由で、チェックサムの不一致が通信エラーに起因するものであっても同様の判断を行う。以上、第1機器101と第2機器102との間での機器認証システムの詳細を説明した。

【0088】尚、本実施の形態1においては、送信データT-Data1及び返信データA-Data2の暗号化対象部はそれぞれ暗号化対象データED及び応答データADであり、チェックサム505及びチェックサム605は含まれていないが、チェックサム505及びチェックサム605も含めて暗号化することができる。

【0089】すなわち、第1機器101の送信データT

ーData 1の作成において、チェックサム対象部CTのチェックサム505を算出した後にチェックサム対象部CTとチェックサム505とを共に共通情報Aにより暗号化する。そして、暗号化されたチェックサム対象部CTとチェックサム505とを含む送信データT-Data 1を第2機器102へ送信する。一方、第2機器102においては、受信した送信データT-Data 1を共通情報Aを用いて復号化して、一連の処理を行った後にランダム情報503により暗号化情報E2とチェックサムCS3とを暗号化して返信データA-Data 2として返信することも可能である。

【0090】以上のように、本実施の形態1に係る機器認証システムにおいては、第1機器101より送信される送信データT-Data 1は、共通情報Aを用いて暗号化されたランダム情報503等を含む暗号化対象データEDとチェックサム505とを含む。そして、第2機器102は、暗号化対象データEDを共通情報Aで復号化して、チェックサム505の一致の判定を行うことにより第1機器101が同一グループに属するか否かの判定を行い、同一グループに属する場合には、ランダム情報503で暗号化された暗号化情報E2、及びチェックサム605を含む返信データA-Data 2を第1機器101へ返送する。次に、第1機器101は、返信データA-Data 2を受信し、保持していたランダム情報503により応答データADの復号化を行い、チェックサム605の一致判定により第2機器102が同一グループに属するか否かの判定を行い、チェックサムが一致する場合には、第2機器102をグループリストに追加する。

【0091】このため、本実施の形態1における機器認証システムにおいて、第1機器101は、共通情報Aを他の機器へ送信することなく同一グループに属する機器のグループリストを自ら作成することができ、認証処理、コンテンツ送受信処理等の第1機器101に負荷の大きい処理を行う前に、安全に同一グループに属する機器のグループリストを取得することができる。

【0092】また、本実施の形態1における機器認証システムにおいては、同一グループに属する機器のグループリスト作成を第1機器101自らがサーバに依らず任意に行うことができ、ブロードキャスト等を行い、複数の機器間における同一グループ化を行う場合に有効となる。

【0093】また、本実施の形態1に係る機器認証システムでは、各端末機器が共通情報Aを有する対等の関係である場合において、各機器は、前記グループリストに従いデータの通信先を決定することにより、コンテンツの取得が不可能な機器に対して通信を行わない。このため、通信網の効率的な利用及びトラフィックの削減等を可能とする。

【0094】さらに、本実施の形態1においては、乱数

であるランダム情報R1を用いて返信データA-Data 2の暗号化及び復号化を行うことにより、より安全に第1機器101及び第2機器102間でのデータ送受信を行うことができ、以前の通信内容を入手して、同じ内容を送信することによって「なりすまし」等を行う攻撃であるリプレイ攻撃等をより効果的に回避することができる。

【0095】尚、ここまで本実施の形態1では機器間で送受信されるデータはメッセージヘッダ501と暗号化された暗号化対象データEDと前記暗号化対象データEDに対するチェックサムとし、受信側である第2機器102でチェックサムの比較判定を行うとして説明した。ここで暗号化対象データEDに予め決められた固定情報を含め、受信側で固定情報が含まれるか否かにより同一の共通情報Aを保持するか否かの判定を行うとしてもよい。即ち、機器間で送受信されるデータとしてはメッセージヘッダ501と固定情報を含む暗号化対象データEDを暗号化したものとしてよい。ここに固定情報を含むとは、例えば、暗号化対象データEDの先頭に「Hello」の文字列を挿入するということである。

【0096】また、本実施の形態1では第2機器102において共通情報Aを用いて同一グループに属するか否かの判定を行っているが、第2機器102において判定を行わず第1機器101においてのみ同一グループに属するか否かの判定を行うとしてもよい。例えば、第2機器102において受信した暗号化情報E1を共通情報Aにより復号しランダム情報R1を取得する。ここでチェックサム判定を行わず（同じ共通情報Aを保持しているかの判定を行わず）、応答データADを前記ランダム情報R1を鍵として暗号化を行い第1機器101に返送する。第1機器101において復号化処理を行い、取得したデータが応答データADとして正しいか否かの判定を行い、同一グループに属するか否かの判定を行うことも可能である。

【0097】（実施の形態2）次に、本実施の形態2に係る機器認証システムについて説明する。尚、本実施の形態2においては、説明を容易にするために、前記実施の形態1と異なる点を中心に説明する。また、本実施の形態2は、デジタル著作物（コンテンツ）と、その利用を可能とする権利情報（ライセンス）とを分離した形態で管理すると共に、ネットワークを介してサーバから端末機器に配信するコンテンツ配信システムに関するものである。本実施の形態2では、同一グループ内の他の端末機器に格納されているライセンスを検索する処理への適用例を示す。

【0098】図10は、本実施の形態2に係る第3機器1001の詳細な構成を示すブロック図である。この第3機器1001は、本実施の形態2においては、前記第1機器101の構成に加えて、コンテンツ利用部1001a、入力部1005、及び検索情報付与部1007を

備えている。

【0099】コンテンツ利用部1001aは、サーバからブロードバンド等のネットワークを介して映画、音楽等のコンテンツ及びライセンスをダウンロードする際に利用され、映画等のコンテンツを記憶するコンテンツ記憶部1002と、端末機器であるPCのユーザ等より発行を依頼されサーバ側において発行されたライセンスを記憶するライセンス記憶部1003とを備え、さらに、コンテンツ記憶部1002に記憶されたコンテンツをライセンスにより許可された利用条件に従って管理するための出力制御部1004を備えている。尚、このコンテンツ利用部1001aの構成は説明のための例示であり、本実施の形態2の構成に限定されるものではない。

【0100】コンテンツ記憶部1002は、端末機器のユーザ側より購入処理を行い、サーバよりブロードバンド等を介してダウンロードされるコンテンツを格納する。このコンテンツは、通常サーバにおいてコンテンツ鍵を用いて暗号化された後に第3機器1001側に送信される。

【0101】ライセンス記憶部1003には、端末機器のユーザ等がサーバに発行依頼して取得するライセンスを保存する。このライセンスは、端末機器に対するコンテンツの利用許可を行うデータであり、また、当該ライセンスが関連付いているコンテンツのコンテンツID、コンテンツの利用形態を定めるアクションID、暗号化されたコンテンツの暗号化を解くコンテンツ鍵等を含み、さらに、コンテンツの機器上での利用条件を示す利用条件データが格納されている。この利用条件データには、有効期限（例えば、2002年6月1日から2002年8月31日）、回数制限（例えば、1回再生が可能）、最大連続再生時間（例えば、1回の再生で最大10時間再生が可能）等の情報が含まれる。尚、サーバで管理する利用条件としては、ライセンスに含まれる利用条件、サーバで管理把握できる情報（例えば、ユーザの利用履歴、ユーザの所持している機器リスト等）となる。

【0102】出力制御部1004は、内蔵又はケーブルを介してテレビ、スピーカー、プリンタ等の再生機器と接続されており、第3機器1001のユーザは、これら再生機器によってライセンスの利用許可範囲内においてコンテンツの利用を行う。また、出力制御部1004と記録機器とを接続して、DVDやSD等の蓄積メディアに対してコンテンツを記録することも可能となる。

【0103】入力部1005は、第3機器1001とネットワークを介して接続され、第3機器1001に備えられるコンテンツ利用部1001aに対して、例えば、コンテンツ、ライセンス、ユーザ情報等の入力を行う。尚、この入力部1005は、データベースを有するサーバ側で管理される。

【0104】端末管理部1001bは、前記実施の形態

1の第1機器101の構成に加えて、検索情報付与部1007を備えている。まず、第3機器1001が他の機器へ送信データT-Data3を送信する場合のデータの流れを説明すると、ランダム情報生成部301及び検索情報付与部1007は、ランダム情報R2及び検索情報Cを生成する。この検索情報Cは、検索対象のライセンスにて利用可能なコンテンツのID及びアクションのIDの情報を含む。尚、検索情報Cには、他の情報を含めることができる。そして、暗号／復号部302は、共通情報Aにより検索情報Cとランダム情報R2とを含む暗号化情報E3を生成し、この暗号化情報E3を機器間通信部305へ送信する。チェックサム生成部304においては、ランダム情報R2と検索情報CとによりCS5を生成し、機器間通信部305は、暗号化情報E3とCS5とを含む送信データT-Data3を第4機器1101へ送信する。

【0105】一方、第3機器1001が他の機器より返信データA-Data4を受信する場合のデータの流れを説明すると、機器間通信部305は、第4機器1101より受信した返信データA-Data4のうち暗号化されたデータE4を復号化するために暗号／復号部302へ送信すると共に、CS7をチェックサム判定部306に送信する。暗号／復号部302は、保持していたランダム情報R2を用いてデータE4の暗号化を解き、復号済み応答データDA4をチェックサム生成部304に送信し、ここで生成されたCS8をチェックサム判定部306へ送信する。チェックサム判定部306では、CS7とCS8との比較を行い、判定の結果CS7とCS8とが一致する場合には、第3機器1001が作成するライセンスリストに第4機器1101が有している検索情報Cに当てはまるライセンスの情報を追加する。

【0106】図11は、本実施の形態2に係る第4機器1101の詳細な構成を示すブロック図である。第4機器1101は、上述した第3機器1001と同様に、コンテンツ利用部1101a、入力部1105、及び端末管理部1101bを備えている。また、コンテンツ利用部1101aは、前記コンテンツ利用部1001aと同様の構成となる。

【0107】端末管理部1101bは、実施の形態1の第2機器102の構成に加えて、検索情報判別部1106を有している。端末管理部1101bが送信データT-Data3を受信してから返信するまでの一連のデータの流れを説明すると、機器間通信部405は、送信データT-Data3を受信し暗号化情報E3を暗号／復号部402へ送り、CS5をチェックサム判定部406へ送信する。暗号／復号部402では、共通情報Aを用いて前記暗号化情報E3の復号化を行い、復号済み暗号化対象データDR2をチェックサム生成部404に送信し、ここで生成されたCS6をチェックサム判定部406に送信する。チェックサム判定部406では、CS5

とCS6との比較を行う。比較の結果、チェックサムが一致しなかった場合には、送信データT-D a t a 3を無視する一方、チェックサムが一致する場合には、検索情報判別部1106は、コンテンツ利用部1101aを検索して検索情報Cに当てはまるコンテンツに対応するライセンスの検索を行う。応答データ生成部407は、検索情報Cを満たすライセンスを発見できない場合には、応答データADを作成しないが、検索情報Cを満たすライセンスを発見した場合には、ライセンス情報C2と応答データADとを含む暗号化情報E4を作成し、機器間通信部405は、この暗号化情報E4とライセンス情報C2及び応答データADから生成したCS7とを含む返信データA-D a t a 4を第3機器1001へ返信する。

【0108】図12は、本実施の形態2に係る送信データT-D a t a 3のデータ構成を示す図である。尚、図12は、本実施の形態2の説明のための例示である。

【0109】送信データT-D a t a 3は、他の機器が第3機器1001と同一グループに属すると共に、検索情報に当てはまるライセンスの検索を行うように要求するメッセージであり、前記実施の形態1で説明した送信データT-D a t a 1の構成に加えて、コンテンツID1201及びアクションID1202のデータを含む。

【0110】コンテンツID1201は、要求するコンテンツのIDを示す。コンテンツには、少なくともコンテンツを一意に特定するための識別子がつけられており、通常、この識別子がコンテンツID1201となる。このコンテンツID1201は、検索対象のライセンスに対応するコンテンツのIDである。

【0111】アクションID1202は、前記コンテンツID1201に示されるコンテンツに対する利用形態を特定する識別子であり、また、検索対象のライセンスにて利用可能なアクションのIDとなる。このアクションとしては、例えば、視聴、再生、コピー、移動、プリント等である。

【0112】尚、これらコンテンツID1201及びアクションID1202は、共通情報Aにより暗号化されてから送信される暗号化対象データEDに含まれ、また、本発明においても前記実施の形態1と同様に暗号化対象データEDのみでなく、チェックサム505も共に共通情報Aにより暗号化して送信することも可能である。

【0113】図13は、本実施の形態2に係る返信データA-D a t a 4のデータ構成を示す図である。この返信データA-D a t a 4は、第3機器1001より送信される送信データT-D a t a 3に対する返信であり、実施の形態1の返信データA-D a t a 2の構成に加えて、ライセンスID1301及び利用条件データ1302が含まれている。

【0114】ライセンスID1301は、権利情報であ

るライセンスそのものではなく、検索情報Cのコンテンツに利用できるライセンスの識別番号であり、本実施の形態2においては、検索対象の端末である第4機器1101で検索されたライセンスを識別するための番号となる。

【0115】利用条件データ1302は、ライセンスにより許可されるコンテンツの利用条件を示すデータであり、通常ライセンスに含まれている。本実施の形態2においては、第3機器1001等で判定される条件でコンテンツの操作内容であるアクション（例えば、視聴）を開始して良いか否かを判定するC条件（例えば、10回）等のデータが含まれている。

【0116】尚、ライセンスID1301及び利用条件データ1302は、ランダム情報R2により暗号化される応答データADに含まれている。

【0117】図14は、本実施の形態2に係る第3機器1001が検索情報Cを用いて第4機器1101及び第5機器1401にライセンス検索を行う際の通信手順を示すシーケンス図である。尚、本図においては、第5機器1401は共通情報Aを有していないものとする。

【0118】まず、第3機器1001は、同一グループ内の他の端末機器に格納されるライセンスを検索し、検索情報Cに含まれるコンテンツのライセンスを保持している機器のライセンスリストを作成することを目的とする。このために、共通情報Aで暗号化した検索情報Cを含む送信データを第4機器1101及び第5機器1401に送信する（ステップ1402）。尚、この送信は、本実施の形態2においてはブロードキャストにより行われている。

【0119】次に、第4機器1101及び第5機器1401は、送信データを受信すると、共通情報Aを用いて送信データのうち暗号化されたデータの復号化を行い、チェックサムの判定を行う（ステップ1403）。送信データを受信した第5機器1401は、共通情報Aを有していないため暗号化された送信データの復号化が正しく行われず、チェックサムの不一致となり返信データは返信されない（ステップ1404）。

【0120】一方、第4機器1101は、共通情報A及び検索情報Cを満たすか否かの判定を行い（ステップ1405）、満たしている場合には返信データにライセンス情報を付与して返信し（ステップ1407）、満たしていない場合には返信しない（ステップ1406）。そして、第3機器1001は、図14に示すように検索情報Cを満たすライセンスリスト1408を作成し、このライセンスリスト1408に従いデータの通信先を決定する。

【0121】図15は、本実施の形態2に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。尚、図9を用いて実施の形態1に係る機器認証システムのグループ判定の処理手順を説明したが、実

施の形態1と同様の処理手順については、図9と同一のステップ番号を付すものとする。以下、図15に従って、第3機器1001が他の機器に対して自らと同一グループに属し、かつ検索情報Cを満たす他の機器のライセンスリスト1408を作成する場合の詳細な流れを説明する。

【0122】最初に、第3機器1001に備えられるランダム情報生成部301は、ランダム情報R2を生成し（ステップ901）、また、検索情報付与部1007は、検索対象のコンテンツID1201及びアクションID1202を有する検索情報Cを生成する（ステップ1501）。そして、ランダム情報R2及び検索情報Cを暗号／復号部302及びチェックサム生成部304に送信する。

【0123】続いて、暗号／復号部302は、ランダム情報生成部301よりランダム情報R2を受信すると共通情報記憶部303に共通情報取得要求を送信し、共通情報記憶部303より共通情報Aを受信し、少なくともランダム情報R2及び検索情報Cを含む暗号化対象データEDを共通情報Aを鍵として暗号化を行い、暗号化情報E3を生成し、機器間通信部305に送信する（ステップ902）。

【0124】次に、チェックサム生成部304は、少なくともランダム情報R2及び検索情報Cを含む暗号化対象データEDに対するCS5を生成し、機器間通信部305に送信する（ステップ903）。

【0125】機器間通信部305は、暗号化情報E3とCS5との両者を受信すると少なくとも前記暗号化情報E3と前記CS5とを含み、通信プロトコルに応じたメッセージヘッダ等を付した送信データT-Data3を他の機器に対して送信する（ステップ904）。

【0126】次に、第4機器1101に備えられる機器間通信部405は、第3機器1001より送信データT-Data3を受信し、送信データT-Data3より前記暗号化情報E3と前記CS5とを抽出する（ステップ905）。そして、機器間通信部405は、暗号化情報E3を暗号／復号部402へ、CS5をチェックサム判定部406へ送信する。

【0127】暗号／復号部402は、暗号化情報E3を受信すると、共通情報記憶部403より共通情報Aを受信する。暗号／復号部402は暗号化情報E3を共通情報Aを鍵として復号化を行い、復号済み暗号化対象データDR2を取得し、チェックサム生成部404に送信する（ステップ906）。続いて、チェックサム生成部404は受信した復号済み暗号化対象データDR2に対するCS6を生成し、チェックサム判定部406へ送信する（ステップ907）。チェックサム判定部406は、受信したCS5とCS6との比較処理を行う（ステップ908）。

【0128】そして、比較処理の結果、チェックサム判

定部406は、CS5=CS6となった場合はチェックサム一致の制御コードを、CS5≠CS6の場合はチェックサム不一致の制御コードを応答データ生成部407に送信する。次に、応答データ生成部407は、チェックサム不一致の制御コードを受信した場合、応答データは生成しない（ステップ909）。

【0129】検索情報判別部1106においては、第3機器1001の送信データT-Data3の検索情報Cに当てはまるコンテンツIDに使用することのできるライセンスを有するか否かの判別を行い、当該ライセンスを有する場合には、ライセンス情報C2を付与した返信データA-Data4の返信を行う（ステップ1502）。また、検索情報Cを満たさない場合には、本実施の形態2においても返信を行わない（ステップ1503）ものとして説明する。尚、返信データA-Data4に検索情報Cに該当するものがないとするデータを記載することも可能である。

【0130】次に、検索情報判別部1106は、ライセンスID等のライセンス情報C2の生成を行い（ステップ1504）、次に、応答データ生成部407は制御コードを受信し、制御コードに応じた前記ライセンス情報C2を含む応答データADを生成し、暗号／復号部402及びチェックサム生成部404に送信する（ステップ910）。

【0131】そして、暗号／復号部402は受信した前記応答データADを保持している復号済み暗号化対象データDR2から前記ランダム情報R2を抽出し、前記ランダム情報R2を鍵としてライセンス情報C2と応答データADとの暗号化を行い、暗号化情報E4を生成し、機器間通信部405に送信する（ステップ911）。また、チェックサム生成部404は受信した応答データADに対するCS7を生成し、機器間通信部405に送信する（ステップ912）。機器間通信部405は、少なくとも暗号化情報E4と前記CS7とを含み、通信プロトコルに応じたメッセージヘッダ等を付した返信データA-Data4を第3機器1001に対して送信する（ステップ913）。

【0132】次に、第3機器1001を構成する機器間通信部305は、前記第4機器1101よりA-Data4を受信し、暗号化情報E4とCS7とを抽出する（ステップ914）。次に、機器間通信部305は、暗号化情報E4を暗号／復号部302へ、CS7をチェックサム判定部306へ送信する。

【0133】暗号／復号部302は、機器間通信部305より暗号化情報E4を受信するとランダム情報生成部301よりランダム情報R2を受信する。暗号／復号部302は、受信した暗号化情報E4を保持していたランダム情報R2を鍵として復号化を行い、復号された暗号化情報（以下、復号済み応答データと呼ぶ）DA4を取得し、チェックサム生成部304及びチェックサム判定

部306に送信する(ステップ915)。続いて、チェックサム生成部304は受信した復号済み応答データDA4に対するCS8を生成し、チェックサム判定部306へ送信する(ステップ916)。チェックサム判定部306は受信したCS7とCS8の比較処理を行う(ステップ917)。

【0134】まず、比較処理の結果、CS7=CS8となった場合は応答データADを送信してきた第4機器1101が同一グループに属し、かつ検索対象のコンテンツに対応するライセンスを有すると判断し、チェックサム判定部306は、第4機器1101が有し検索対象となるライセンスをライセンスリスト1408に追加する(ステップ1505)。CS7≠CS8の場合は同一グループに属しないか、又は検索情報Cを満たさないと判断する(ステップ918)。尚、本実施の形態2においては、送信データT-Dat a 3及び返信データA-Dat a 4の暗号化対象部はそれぞれ暗号化対象データED及び応答データADであるが、チェックサム505及びチェックサム605も含めて暗号化することができるのは言うまでもない。

【0135】以上のように、本実施の形態2に係る機器認証システムにおいては、第3機器1001より送信される送信データT-Dat a 3は、ランダム情報503に加えて検索情報CであるコンテンツID1201及びアクションID1202を含む。そして、第4機器1101は、暗号化された暗号化対象データEDを共通情報Aで復号化して、チェックサム505を比較判定することにより第3機器1001が同一グループに属するか否かの判定を行い、同一グループに属する場合には、さらに、検索情報判別部1106において、前記コンテンツID1201及びアクションID1202の検索対象となるコンテンツに適したライセンスを有しているか否かの判定を行い、判定の結果、検索情報Cを満たすライセンスを有する場合には、ライセンスID1301、利用条件データ1302等を含む返信データA-Dat a 4を第3機器1001へ返送する。

【0136】そして、第3機器1001は、前記返信データA-Dat a 4を受信し、応答データADをランダム情報503により復号化して、チェックサム605の一致判定を行うことにより、第4機器1101が同一グループに属し、かつ検索情報Cを満たすライセンスを有すると判断し、検索情報Cを満たすライセンスリスト1408を作成する。

【0137】このため、前記実施の形態1の作用効果に加えて、本実施の形態2における機器認証システムにおいては、第3機器1001よりブロードキャストにより送信された送信データT-Dat a 3を受信した機器全てが返信データA-Dat a 4を返信するのではなく、同一グループに属し、かつ検索情報Cを満たすライセンスを有する機器のみが返信データA-Dat a 4を返信

する。このため、第3機器1001は、検索対象のライセンスを有する機器のライセンスリスト1408を作成して、このライセンスリスト1408に従うことによりライセンスの交換、購入等が可能な他の機器をより効率的に特定することができる。従って、本発明は、コンテンツ配信システムにおける端末機器間でのライセンス検索に適用することが可能である。

【0138】尚、上述した各実施の形態において、共通情報は、共通情報Aを用いて説明したが、各機器が複数の共通情報も保持し、これら複数の共通情報を追加、削除等することにより、同一グループ範囲の設定についても柔軟かつ容易に実現できるようにすることも可能である。

【0139】

【発明の効果】以上の説明から明らかなように、本発明に係る機器認証システムにおいては、少なくとも第1及び第2機器から構成され、前記第1及び前記第2機器が同一のグループに属するか否かを判定する機器認証システムであって、前記第1機器は、共通情報を記憶する第1共通情報記憶手段と、鍵情報を含む送信データを生成する送信データ生成手段と、生成された送信データを前記共通情報で暗号化する第1暗号化手段と、前記第1暗号化手段で得られた暗号化送信データを前記第2機器に送信する第1送信手段と、前記第2機器から送られてきた暗号化返信データを前記鍵情報で復号化する第1復号化手段と、復号化された前記返信データが一定の規則を有するか否かを判定し、一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断する認証手段とを備え、前記第2機器は、共通情報を記憶する第2共通情報記憶手段と、前記第1機器から送られてきた暗号化送信データを前記共通情報で復号化する第2復号化手段と、復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、前記送信データが一定の規則を有する場合に、前記第1及び第2機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第2暗号化手段と、前記第2暗号化手段で得られた暗号化返信データを前記第1機器に送信する第2送信手段とを備える。

【0140】これによって、本発明に係る機器認証システムにおいては、各端末機器も対等の関係になる場合において同一グループに属する機器の特定を可能とし、また、端末機器が認証処理、コンテンツ送受信処理等の端末に負荷の大きい処理を行う前に、安全に同一グループに属する端末のグループリストを取得し、さらに、前記グループリストを利用することにより、送信データの送信先となる機器を決定して、コンテンツの取得が不可能な端末に対しては通信を行わずに、通信経路の効率的な利用等を可能とする。

【0141】また、本発明に係る機器認証システムにおいては、前記送信データ生成手段は、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、前記第2機器は、さらに、復号化された前記送信データに含まれる検索情報が示す物を当該第2機器が保持するか否か判定する検索情報判定手段を備え、前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成する。そして、前記送信データ生成手段は、デジタルコンテンツを特定するコンテンツIDを前記検索情報として前記送信データに含ませ、前記返信データ生成手段は、前記送信データに含まれているコンテンツIDが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第2機器が保持する場合に、当該ライセンスを特定するライセンスIDを前記返信データに含ませる。

【0142】これらにより、本発明に係る機器認証システムにおいては、検索対象のライセンスを有する機器のライセンスリストを作成して、このライセンスリストに従うことによりライセンスの交換、購入等が可能な他の機器をより効率的に特定して、コンテンツ配信システムにおける端末機器間でのライセンス検索に適用することを可能とする。

【図面の簡単な説明】

【図1】実施の形態1に係る機器認証システムを説明する概略図である。

【図2】実施の形態1に係る複数の機器とグループとの関係を示す図である。

【図3】実施の形態1に係る第1機器の詳細な構成を示すブロック図である。

【図4】実施の形態1に係る第2機器の詳細な構成を示すブロック図である。

【図5】実施の形態1に係る送信データのデータ構成を示す図である。

【図6】実施の形態1に係る返信データのデータ構成を示す図である。

【図7】(a)は、実施の形態1におけるユーザインターフェイスの画面を示す図である。(b)は、実施の形

態1における別のユーザインターフェイスの画面を示す図である。

【図8】(a)は、実施の形態1における第1機器が作成するグループリストの情報項目を示す図である。

(b)は、実施の形態1における第1機器が作成する別のグループリストの情報項目を示す図である。

【図9】実施の形態1に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。

【図10】実施の形態2に係る第3機器の詳細な構成を示すブロック図である。

【図11】実施の形態2に係る第4機器の詳細な構成を示すブロック図である。

【図12】実施の形態2に係る送信データのデータ構成を示す図である。

【図13】実施の形態2に係る返信データのデータ構成を示す図である。

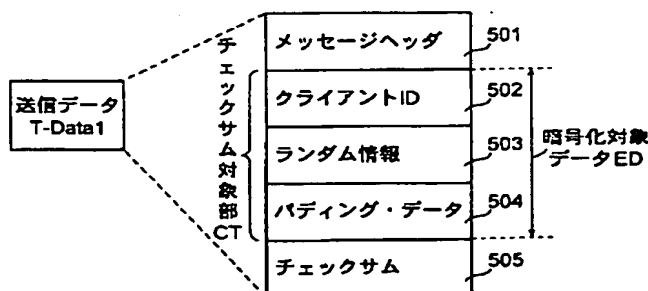
【図14】実施の形態2に係る第3機器が検索情報を用いて第4機器及び第5機器にLT検索を行う際の通信手順を示すシーケンス図である。

【図15】実施の形態2に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。

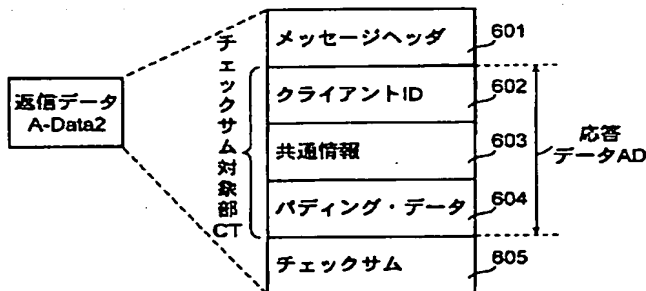
【符号の説明】

- 101 第1機器
- 102 第2機器
- 301 ランダム情報生成部
- 302, 402 暗号/復号部
- 303, 403 共通情報記憶部
- 304, 404 チェックサム生成部
- 305, 405 機器間通信部
- 306, 406 チェックサム生成部
- 407 応答データ生成部
- 1001 第3機器
- 1001a, 1101a コンテンツ利用部
- 1001b, 1101b 端末管理部
- 1005, 1105 入力部
- 1007 検索情報付与部
- 1101 第4機器
- 1106 検索情報判別部

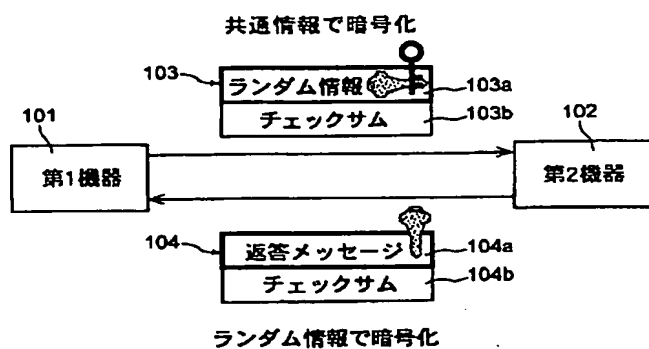
【図5】



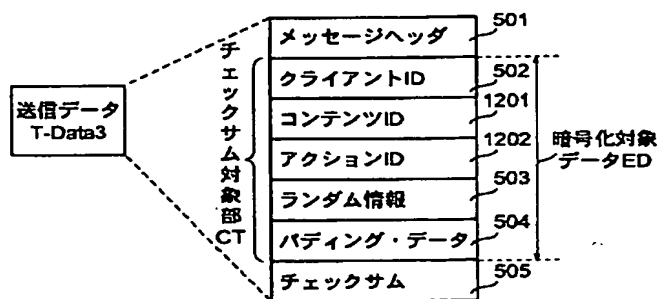
【図6】



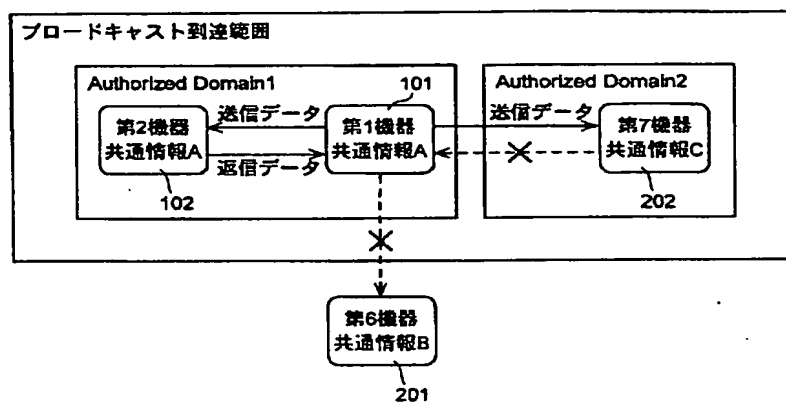
【图 1】



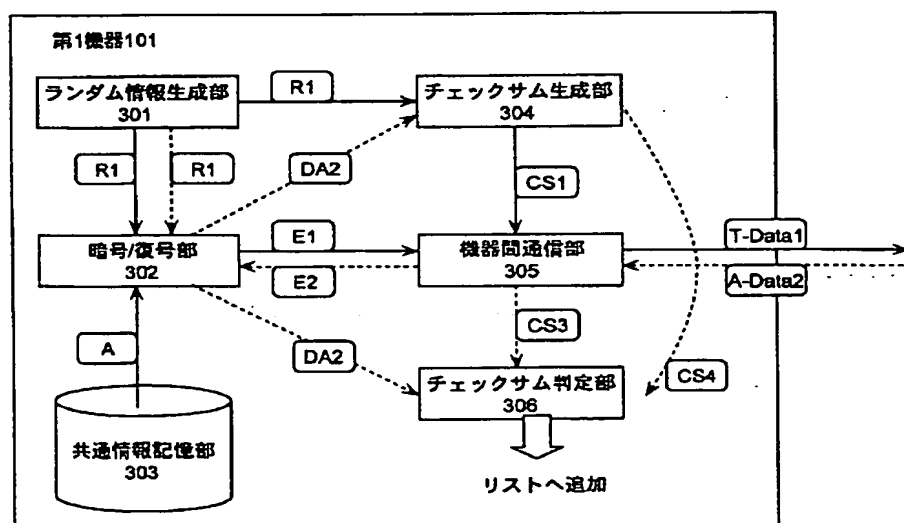
【图 1 2】



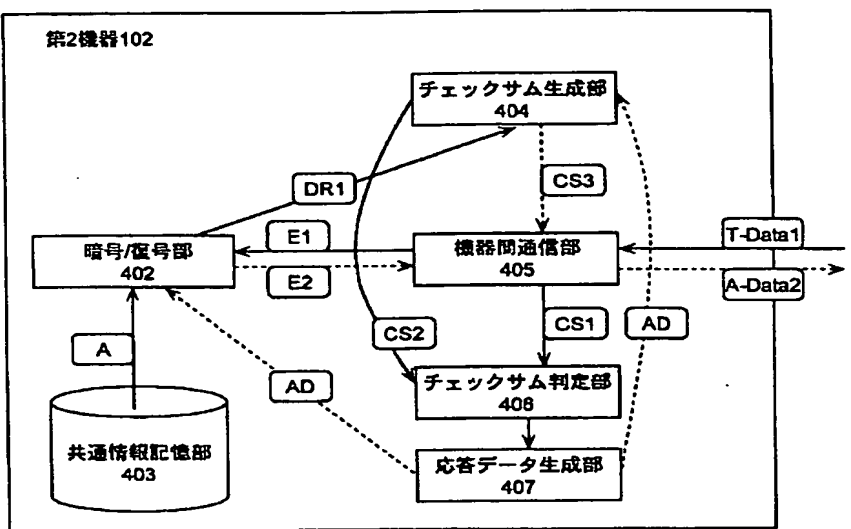
【图2】



【図 3】



【図4】



【図7】

(a)

【共通情報設定画面例】

共通情報の設定
新規に設定する共通情報と、本機器に設定するためのパスワードを入力してください。

共通情報

パスワード

OK

(b)

【共通情報表示例】

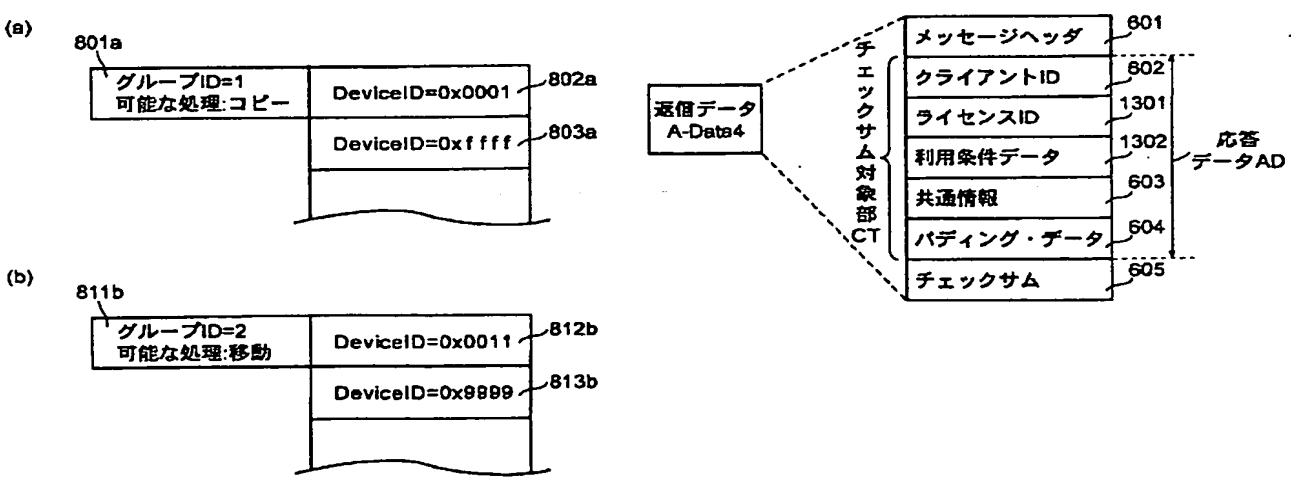
共通情報の表示
本機器に設定されている共通情報は

zeppetstore

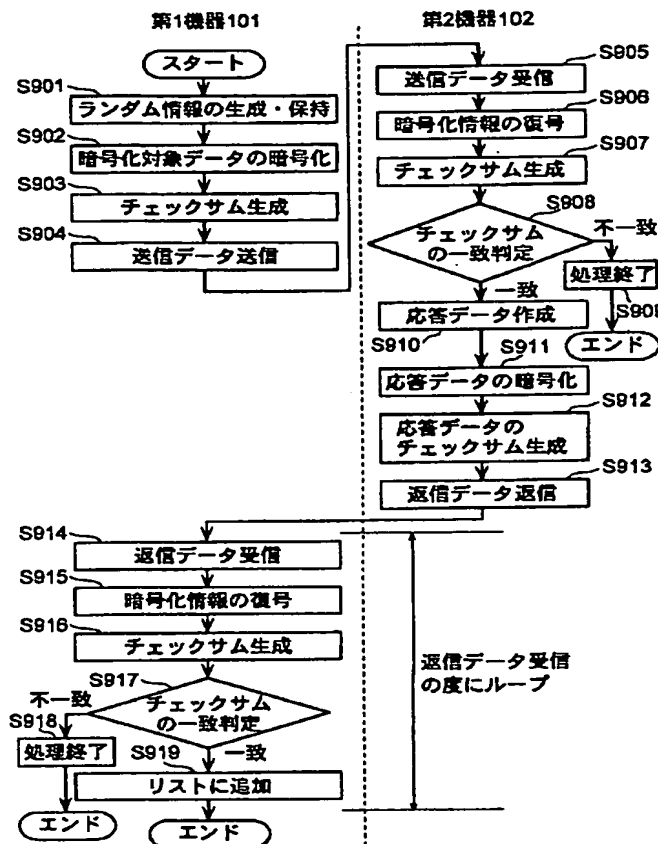
です。

【図8】

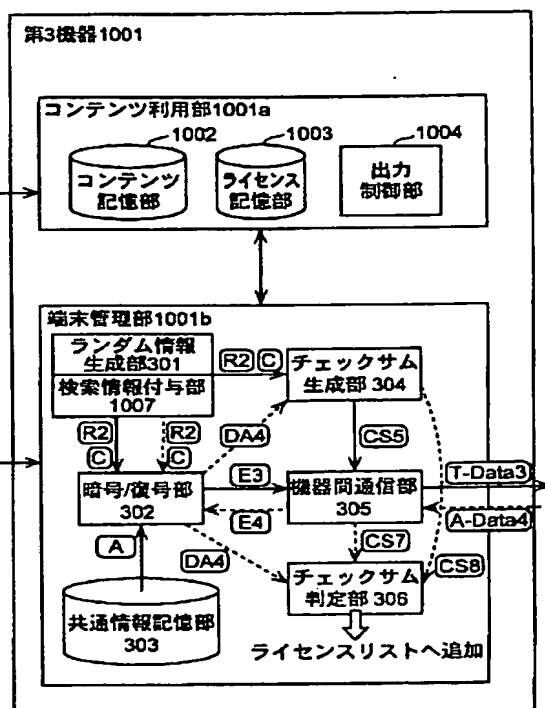
【図13】



【図9】

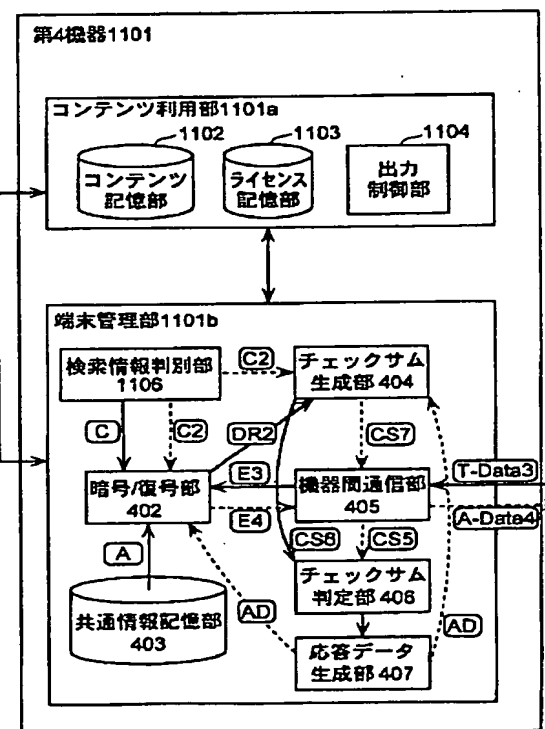
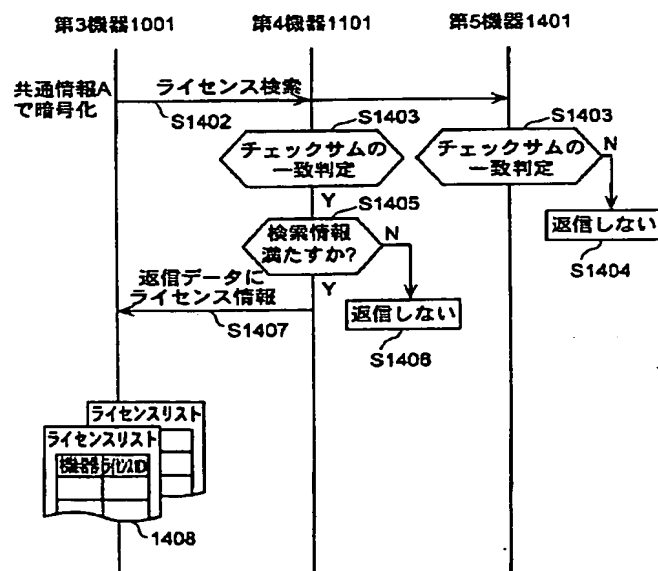


【図10】

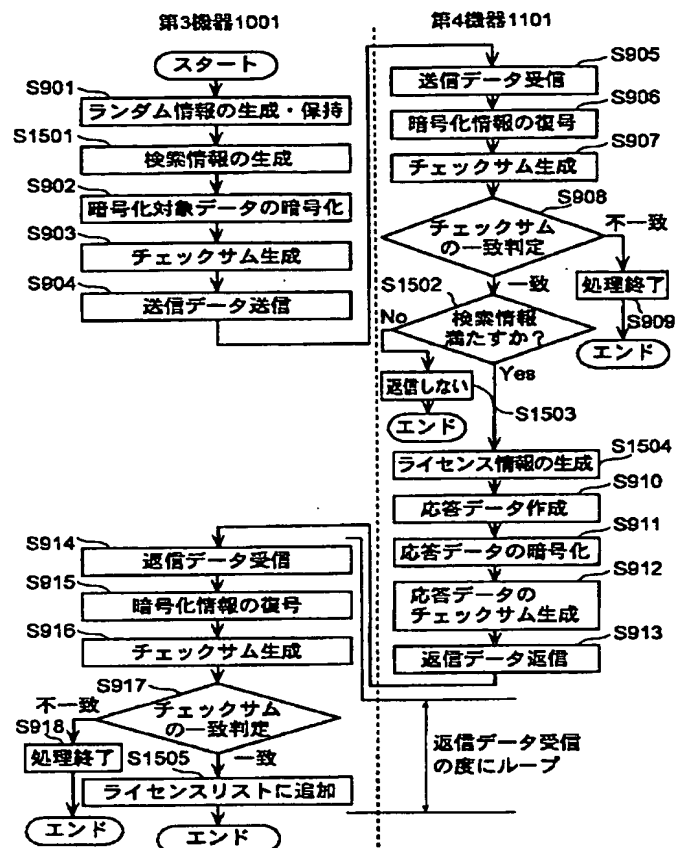


【図11】

【図14】



【図15】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テーマコート* (参考)

H 0 4 L 9/00

6 0 1 E

(72) 発明者 中原 徹

大阪府門真市大字門真1006番地 松下電器
産業株式会社内F ターム(参考) 5B085 AA08 AE06 AE23 BG01 BG02
BG07
5J104 AA07 AA16 EA04 EA16 EA18
GA05 KA02 KA04 KA06 NA02
PA07